UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/040,770 | 12/28/2001 | Lester J. Chong | PD-201133 | 2129 |

20991 7590 04/23/2008

THE DIRECTV GROUP, INC.
PATENT DOCKET ADMINISTRATION
CA / LA1 / A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

| EXAMINER | |
|---|---|
| NEURAUTER, GEORGE C | |
| **ART UNIT** | **PAPER NUMBER** |
| 2143 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/23/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* LESTER J. CHONG, MICHAEL MAKAIJANI,
and DOUGLAS CHELINE

---

Appeal 2008-0067
Application 10/040,770
Technology Center 2100

---

Decided: April 23, 2008

---

*Before* JAY P. LUCAS, THU A. DANG, and STEPHEN C. SIU,
*Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

## DECISION ON APPEAL

## I. STATEMENT OF CASE

Appellants appeal the Examiner's final rejection of claims 1-12 and 14-19 under 35 U.S.C. § 134(2002). We have jurisdiction under 35 U.S.C. § 6(b)(2002).

## A. INVENTION

According to Appellants, the invention is a system for content filtering including at least one content server that stores content. The system also includes at least one client computer configured to transmit a request for the content to the at least one content server. The request contains an address of the content server and a port number associated with such a request for the content. A gateway is coupled to the at least one client computer. The gateway is configured to receive and renumber the request with a new rarely used port number associated with a filter privilege of a user of the at least one client computer. The system also includes a content filtering server configured to block restricted content based on the filter privilege. Finally, a switch is coupled to the gateway, the content filtering server, and the content server. The switch is configured to listen for the request on the rarely used port number and to redirect the request to the content filtering server (Spec., Abstract.)

## B. ILLUSTRATIVE CLAIM

Claim 1 is exemplary and is reproduced below:

1. A method for content filtering, comprising:

receiving a request for content from a client computer, where said request includes a port number assigned to an application program running on said client computer;

determining that said port number is a predetermined port number associated with the request for content;

renumbering said request with a new port number;

transmitting said request with said new port number to a content filtering server that is configured to listen for requests on said new port number; and

obtaining from said content filtering server an indication of whether said content is restricted based on said request and said new port number.

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Freund US 2003/0055962 A1 Mar. 20, 2003
(Filed Aug. 30, 2001)

SonicWall, "SonicWALL SOHO Internet Security Appliance," document revision A, part # 232-000019-00, 1999.

Claims 1-6, 11, 12, 14, 15, and 17-19 stand rejected under 35 U.S.C. § 102(e) over the teachings of Freund; and

Claims 7-10, and 16 stand rejected under 35 U.S.C. § 103(a) over the teachings of Freund, and SonicWall.

We affirm.

## II. ISSUES

The issues are whether Appellants have shown that the Examiner erred in finding that:

(A) claims 1-6, 11, 12, 14, 15, and 17-19 are unpatentable under 35 U.S.C. § 102(e) over the teachings of Freund; and

(B) claims 7-10, and 16 are unpatentable under 35 U.S.C. § 103(a) over the teachings of Freund, and SonicWall.

## III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

### *Freund*

1. Freund discloses verifying that a computer is in compliance with established security policies. If a computer is not in compliance, then the computer's access to the Internet is restricted to those activities necessary to get the computer back into compliance. The security solution only permits an Internet connection to a sandbox server for the limited purpose of informing the user of the non-compliance and enabling the user to take the steps necessary to bring his or her computer into compliance (pg. 7, para. [0071]).

2. In Freund, routing component 313 redirects non-compliant computer 330 which is permitted only a limited Internet connection to sandbox server 360. (pg. 8, para. [0078]; Fig. 3).
3. The sandbox server operates by looking for communications on certain port addresses and using the port address as a response code. The different port addresses can, in effect, indicate a certain problem or condition. For example, port 8082 means no client response was received. Other ports can be used to indicate other specific problems (pg. 9, para. [0095]). In the implementation of the sandbox server, the server listens to various ports and responds by displaying HTTP pages in response to communications on various ports (pg. 11, para [0117]).
4. In the operation for the router-side security module, in step 910, a connection attempt from one of the local computers to the Internet is received by the router (pg. 14, para. [0147]; Fig. 9).
5. If the table entry is compliant, then the client computer is permitted to access the Internet. If not, then the routing component proceeds to step 950. In step 950, the routing component determines whether or not the destination port is HTTP (port 80 TCP). If the destination port is HTTP, then the re-routing manager proceeds in step 951 to manipulate the destination IP address and port (pg. 14, para. [0148]; Fig. 9).
6. In step 951, if the entry in the router compliance table is less than 256, then the destination port is set to the value of the table entry plus

8080. For example, if the table entry is 1, the destination port is set to port 8081 (which represents 8080 plus 1). This also conveys information to the sandbox server in the HTTP header permitting the sandbox server to categorize the reason for non-compliance. Using this information, the sandbox server then displays a page with information enabling the client to address the specific problem that was detected. In this manner, the connection request from a non-compliant client computer is patched and manipulated to reroute this packet to the sandbox server (pg. 14, para. [0149]; Fig. 9).

*SonicWall*

7. SonicWall discloses an authentication mechanism which gives authorized users access to the LAN from remote locations on the Internet as well as a means to bypass the content filtering and blocking from the LAN to the Internet (pg. 101, ll. 1-10).

## IV. PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 102, a single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation. *Perricone v. Medicis Pharm.,* 432 F.3d 1368, 1375-76 (Fed. Cir. 2005) (citation omitted). "Anticipation of a patent claim requires a finding that the claim at issue 'reads on' a prior art reference." *Atlas Powder Co. v. IRECO, Inc.*, 190 F.3d 1342, 1346 (Fed Cir. 1999) ("In other words, if granting patent protection on the disputed claim

would allow the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art.") (citations omitted).

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

The *claims* measure the invention. *See SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). "[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)). Our reviewing court has repeatedly warned against confining the claims to specific embodiments described in the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc).

In the absence of separate arguments with respect to claims subject to the same rejection, those claims stand or fall with the claim for which an

argument was made. *See In re Young,* 927 F.2d 588, 590 (Fed. Cir. 1991). *See also* 37 C.F.R. § 41.37(c)(1)(vii)(2004).

## V. ANALYSIS

### *35 U.S.C. § 102(e)*

Appellants argue that Appellants can find no teaching or suggestion in Freund of "the step of receiving a request for content from a client computer, where said request includes a port number assigned to an application program running on the client computer" (App. Br. 7-8). Appellants assert that Freund is "significantly different than the present application" because Freund "describes the operation for a router-side security module" (App. Br. 7), and that "Freund is directed to security issues and not for restricting access" (App. Br. 8).

We disagree. The Examiner's position as to Freund disclosing the claimed elements on appeal beginning at page 4 of the Answer and the Examiner's corresponding responsive arguments beginning at page 15 of the Answer meet all of the limitations required by independent claims 1, 14, 18, and 19 on appeal.

Appellants' arguments that Freund is "significantly different than the present application" because Freund "describes the operation for a router-side security module," and that "Freund is directed to security issues and not for restricting access" are not commensurate with the invention that is claimed. That is, Appellants appear to be arguing that Freund does not disclose receiving a request for content which includes a port number

assigned to an application program because Freund is directed to security issues, which is not commensurate with the claimed invention.

Freund discloses a request for connection to the Internet (FF 4). As set forth in the Appeal Brief, "Appellants admit that a router receives a request for connection to the Internet from a local computer" (App. Br. 7). We thus agree with the Examiner that Freund discloses "a request for content from a client using a Web browser to a server which contains content" (Ans. 18).

In Freund, the routing component determines whether or not the destination port is HTTP, i.e., determines whether the port number is predetermined port 80 TCP (FF 5). The Examiner found that the port number of Freund is "a port number assigned to an application program running on said client computer." As the Examiner set forth on page 19 of the Answer, "the Examiner has reasonably interpreted this limitation in its broadest sense wherein the application program is assigned its well known port number." The Examiner added that, in Freund, "HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands." We agree with the Examiner that such TCP port number 80 assigned to HTTP is a port number assigned to an application program.

In the Reply Brief, Appellants do not argue these findings by the Examiner. Instead, Appellants argue that "it is clear that the security issues and not a request for content is the primary focus of the Freund reference,"

(Reply Br. 3) and add the argument that, due to this difference in focus, "there is no request for content and no request for content includes a port number assigned to an application program" (Reply Br. 4).

Appellants' argument that Freund differs from the claimed invention because the primary focus is "the security issues" is not commensurate with the claimed invention. The "request for content" cannot be confined to a specific embodiment. Appellants' claims simply do not place any limitation on what the "request for content" is to be, to represent, or to mean, other than that the request for content is from a client computer, and includes a port number assigned to an application program.

We agree with the Examiner's position as to Freund disclosing the "request for content" beginning at page 4 of the Answer and the Examiner's corresponding responsive arguments beginning at page 15 of the Answer. The Examiner found that Freund discloses "a request for content from a client using a Web browser to a server which contains content" (Ans. 18). As set forth in the Answer, the Examiner's "broadest reasonable interpretation of the claim wherein the request includes a port number that is assigned to an application program running on the client computer or a 'web browser' as described in Freund that uses the HTTP protocol to request and retrieve content is valid" (Ans. 20).

In Freund, a request from a local computer for connection to the Internet is received by the router wherein the routing component determines whether or not the port number is port 80 TCP (FF 5-6). We agree with the

Examiner that such a request to the router is a request for content which includes a port number assigned to an application program.

Appellants also argue that Freund's sandbox server "is not a content filtering server" (App. Br. 8) and thus "it appears that transmitting the request with the new port number to a content filtering server that is configured to listen for requests on the new port number is not taught or suggested" by Freund (App. Br. 9).

However, the "content filtering server" cannot be confined to a specific embodiment. Appellants' claims simply do not place any limitation on what the "content filtering server" is to be, to represent, or to mean, other than that the server is configured to listen for requests on a new port number.

We agree with the Examiner's position as to Freund disclosing such a "server" beginning at page 4 of the Answer and the Examiner's corresponding responsive arguments beginning at page 22 of the Answer.

Freund discloses that the sandbox server operates by looking for communications on certain port addresses and using the port address as a response code, wherein the different port addresses can, in effect, indicate a certain problem or condition, and wherein the server listens to various ports and responds by displaying HTTP pages in response to communications on various ports (FF 1-3). In Freund, connection requests from non-compliant client computers are rerouted to the sandbox server (FF 6). We agree with the Examiner that Freund discloses the recited limitation of a server "that is configured to listen for requests on the new port number."

In the Reply Brief, Appellants add the argument that "the Examiner fails to appreciate the last two steps of claim 1" which "recites 'whether said content is restricted based on the request and the new port number'" (Reply Br. 4). However, the Examiner found that Freund discloses such claimed limitation as set forth in the Examiner's position at page 4 of the Answer and the Examiner's corresponding responsive arguments beginning at page 22 of the Answer.

In Freund, information is conveyed to the sandbox server in the HTTP header indicating that the port number is set to 8081, permitting the sandbox server to categorize the reason for non-compliance, as well as connection requests from the non-compliant client computers (FF 6). If a computer is not in compliance, then the computer's access to the Internet is restricted to those activities necessary to get the computer back into compliance (FF 1).

The Examiner found that Freund's determination of whether access to the Internet is restricted is the claimed "indication of whether content is restricted." Appellants provide no argument to dispute that the Examiner has correctly shown where all these claimed elements appear in the prior art. We conclude that the Appellants have not shown that the Examiner erred in finding that Freund discloses the claimed content restriction of claim 1.

Similarly, as to the other recited elements of claim 1, Appellants provide no argument to dispute that the Examiner has correctly shown where all these claimed elements appear in the prior art. Thus, we deem those arguments waived. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2004).

Accordingly, we conclude that the Appellants have not shown that the Examiner erred in rejecting claim 1 under 35 U.S.C. § 102(e). Appellants do not provide a separate argument for independent claims 14, 18, and 19, and thus, claims 14, 18, and 19 fall with claim 1.

As to claims 2-6, 11, 12, 15, and 17 depending from claims 1 or 14, Appellants provide no argument to dispute that the Examiner has correctly shown where all the claimed elements appear in the prior art.

In the Reply Brief, Appellants add the argument regarding claims 2-3 that "Appellants… find no teaching for a client computer's filter privilege" in Freund, because "There is no indication of restricting content" (Reply Br. 5). However, the Examiner found that Freund discloses such claimed limitations as set forth in the Examiner's position at page 5 of the Answer and the Examiner's corresponding responsive arguments beginning at page 26 of the Answer.

As discussed above, in Freund, if a computer is not in compliance, then the computer's access to the Internet is restricted to those activities necessary to get the computer back into compliance (FF 1). We agree with the Examiner that such access restriction to the Internet is a filtering of content to a client computer.

Accordingly, we conclude that the Appellants have not shown that the Examiner erred in rejecting claims 2-6, 11, 12, 15, and 17 under 35 U.S.C. § 102(e).

*35 U.S.C. § 103(a)*

As to claims 7-10, and 16, Appellants repeat the argument that in Freund, Appellants "can find no teaching or suggestion for content filtering" (App. Br. 15). As discussed above, Freund discloses restricting a computer's access to the Internet (FF 1), and we agree with the Examiner that such access restriction to the Internet is content filtering. Though the Appellants added in the Reply Brief the argument that SonicWall's "bypass filter" is not a "content filter" (Reply Br. 6), we agree with the Examiner that Freund discloses such filter.

As to the other recited elements of claims 7-10, and 16, Appellants provide no argument to dispute that the Examiner has correctly shown where all these claimed elements appear in Freund and SonicWall. Thus, we deem those arguments waived. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2004).

Accordingly, we find that the Appellants have not shown that the Examiner erred in rejecting claims 7-10, and 16 as unpatentable over Freund and SonicWall under 35 U.S.C. § 103(a).

CONCLUSIONS OF LAW

(1) Appellants have not shown that the Examiner erred in finding claims 1-6, 11, 12, 14, 15, and 17-19 unpatentable under 35 U.S.C. § 102(e) over the teachings of Freund.

(2) Appellants have not shown that the Examiner erred in finding claims 7-10, and 16 unpatentable under 35 U.S.C. § 103(a) over the teachings of Freund and SonicWall.

(3) Claims 1-12 and 14-19 are not patentable.

DECISION

The Examiner's rejections of claims 1-6, 11, 12, 14, 15, and 17-19 under 35 U.S.C. §102(e) and claims 7-10, and 16 under 35 U.S.C. §103(a) are affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

rwk

THE DIRECTV GROUP, INC.
PATENT DOCKET ADMINISTRATION
CA / LA1 / A109
P O BOX 956
EL SEGUNDO CA 90245-0956